REMARKS

By this amendment, claims 24-26 and 39 are pending, in which claims 20-23, 27-38 and 40 were withdrawn from consideration. Claims 1-19 were previously canceled. No claims are currently amended or newly presented.

The final Office Action mailed April 27, 2007 rejected claims 24-26 and 39 under 35 U.S.C. § 102 as anticipated by *Fransdonk.* (US Patent Application Publication No. 2006/0210084 A1).

Applicants respectfully traverse the outstanding anticipation rejection on the merits, because thc claimed invention patentably defines over the applied prior art (*Fransdonk*), as next discussed.

For example, independent claim 24 recites "**creating** a **unique user key using system information of a user terminal**; and transmitting digital information and user information including the unique user key to a server system via a network, wherein the **unique user key is transmitted by a user application tool installed in the user terminal for authentication**." The Office Action, on page 4, cites to various paragraphs 0105, 126, 146, 183, 202 and 210-221 of *Fransdonk*, for a supposed disclosure of the above claimed features. Applicants respectfully disagree, as the claim language is taken out of context. Although *Fransdonk* uses the term "unique user key," *Fransdonk* does not disclose any capability for "creating a unique user key using system information of a user terminal" and "unique user key is transmitted by a user application tool installed in the user terminal for authentication" in the manner claimed. The cited passages are provided as follows (Emphasis Added):

> [0105] The table MerchantUser represents the users (operators) of content providers 16. They possess a secure token to access the conditional access server 36. This table is used to verify the identity of the content providers 16 when he or she logs on to the system.

Field	Description
Serial	**Secure device serial number**
MerchantId	Content provider ID linked with the secure device
EMail	E-mail address of user
UserName	(Optional) name of the user
AccessRights	Integer representing user's access rights. This allows a way to distinguish the access rights of a certain user (for example: A user is allowed access to certain applications only).
SecretKey	
PublicKey	

Serial is the unique key.

[0126] Turning now to the gateway function performed by a conditional access agent 28, after a subscriber (or user) has been granted access to the content, a request is sent to the local content server 40 to \`release\` the content. This request contains all the necessary data, including the IP destination address/port, subscriber signed access criteria, the subscriber certificate and the key to decrypt the content (encrypted with the public key or secret group key of the conditional access agent 28). **The content is then decrypted, watermarked and optionally re-encrypted with a different key (e.g., a unique user key).**

[0146] An exemplary operational scenario involving the conditional access agent 28 will now be described with reference to FIG. 5:

[0183] A further advantage is that **personal re-encryption of content (e.g., utilizing a unique user key)** requires that an unauthorized distributor redistribute the entire content, as opposed to just relevant keys.

[0202] If the request passes the verification process, **the conditional access agent 28 then establishes a secure session with the conditional access client 48, and generates a unique user key (U_k).** The unique user key (U_k) is then encrypted with a public key of a copy-protected device associated with the secure device 46, and communicated to the conditional access client 48 using the secure session. If a copy-protected device is not available, and not required according to the access criteria, the unique user key may be encrypted utilizing a public key of the secure device 46.

[0210] Having performed the operation relating to the content, **the conditional access agent 28**, again within the secure tamper-proof environment, **generates a unique user key (U_k)**, and re-encrypts the content with this unique user key.

[0211] As all operations within block 154 are performed within the secure, tamper-proof environment, it will be appreciated that the interests of the content provider 16 are well protected, and that the product key is not exposed outside the secure environment. Further, only an authorized entity (e.g., a specific conditional access agent 28) is authorized to reveal the product key within thc secure environment as the private key of a secure device of the agent 28 is required to decrypt the product key. In this way, the content provider 16 exercises strict and rigorous control of which entity is able to decrypt the product key.

[0212] In one exemplary embodiment, at block 156, the content distributor 20, utilizing the conditional access agent 28 and within the secure tamper-proof environment, encrypts the product key with the unique user key (U_k). The content distributor 20 then also encrypts the unique user key with a public key of the content destination 22. At block 158, the content distributor 20 transmits the encrypted content, the encrypted product key, and the encrypted unique user key to the content consumer at a content destination 22.

[0213] At block 160, the content consumer at the content destination 22 decrypts the unique user key utilizing a private key of the secure device 46, then dccrypts the product key utilizing the unique user key, and finally decrypts the watermarked content utilizing the decrypted product key.

[0214] As discussed above, the method 150 is particularly advantageous in that it enables a content provider 16 to authorize a specific content distributor 20 to perform an operation relating to the content, and in one embodiment, to contribute to combating authorized distribution. Such operations may include, for example, watermarking or further encryption of the content. In addition to the authorization being specific to a content distributor 20, the method 150 is also advantageous in that the operation is performed in a secure, tamper-proof environment within which the interests of the content provider 16 are protected and the product key is subject to very limited and controlled exposure.

[0215] In this way, a content provider 16 is provided with assurances that distributed secure agents (e.g., conditional access agents 28) located at various distribution points operate to protect the interests of the content provider 16. The content provider 16 is thus provided with a degree of security and assurance regarding operations that are performed by content distributors 20 and the content provider 16 is thus likely to entrust distribution of sensitive and very valuable content to such a content distributor 20.

[0216] Further, by performing the operation at block 154 (e.g., watermarking or encrypting) prior to actual delivery of the content to a consumer (i.e., within the network), the risks of piracy are reduced. Upgrades to a secure agent (e.g., the conditional access agent 28) are also more easily implemented than upgrades to processes at consumer locations.

[0217] In conclusion, the method 150 enables an association operation (e.g., a watermarking process) to be distributed to content distributors 20 located at ISPs and therefore closer to content consumers. This is advantageous in that it enables load management. The method 150 also addresses concerns of a content provider 16 regarding security resulting from that, in order to perform certain operations on the content (e.g., a watenmarking operation) at a distributor 20, the content must "be in the clear" in order to properly perform the operation. The method 150 addresses this concern by providing a secure environment in which the operation is performed, and providing the content provider 16 with control over which content distributors 20 are authorized to generate clear content within the secure, tamper-proof environment with the purposes of performing such operations.

[0218] So-called "key hook piracy" occurs when an authorized, but fraudulent, user distributes decryption keys, that may be utilized to decrypt content to unauthorized users. Distributing such a single decryption key over networks, such as the Internet, can be done effectively.

[0219] FIGS. 8A and 8B are block diagrams illustrating, at a high level, a method, according to an exemplary embodiment of the present invention, of combating "key hook piracy". With specific reference to FIG. 8A, the present invention proposes encrypting clear content 24 with a relatively large number of session keys 98 to generate encrypted content 26. In one embodiment, the session keys 98 comprise a sequence of random, time-varying session keys.

[0220] FIG. 8B illustrates further details regarding the distribution of content and the session keys 98, according to an exemplary embodiment of the present invention. The content provider 16 is shown to firstly distribute encrypted content 26 (i.e., clear content 24 encrypted with the session keys 98). In one embodiment, the content provider 16 may distribute the encrypted content 26 directly to a content destination 22. In an alternative embodiment, the encrypted content 26 may be distributed to a local content server 40 at a content distributor 20, and cached by the local content server 40 for eventual distribution to a content destination 22.

[0221] The conditional access server 36 at the content provider 16 also operates to encrypt each of the session keys of the sequence of the time-varying session keys with a product key (S_p), and to distribute the encrypted session keys to the conditional access agent 28, as indicated at 104. The conditional access server 36 also operates to encrypt the product key (S_p) with the public key of a specific conditional access agent 28, and then to distribute the encrypted product key to the specific conditional access agent 28, as indicated in FIG. 8B at 106. During delivery to a conditional access client 48, **the conditional access agent 28 replaces the session keys encrypted with the product key (S_p) with session keys encrypted with a unique user key (U_k), instead of the product key (S_p).** Specifically, prior to deliver to a conditional access client 48, the conditional access agent 28 decrypts the encrypted product key received from the conditional access server 36 utilizing the private key (or secret key) of the conditional access agent 28, decrypts the sequence of session keys encrypted with the product key,

> and then re-encrypts the sequence of session keys utilizing the unique user key (U_k). The re-encrypted sequence of session keys is then distributed from the conditional access agent 28 to the conditional access client 48, as indicated at 108. **The conditional access agent 28 also distributes the unique user key (U_k) to the conditional access client 48 via a secure authorization channel, as indicated in FIG. 8B at 110.**

The above cited passages describe the operation of two distinct processes in the *Fransdonk* system, that of the distribution process 12 and the delivery process 14 (*see* FIG. 1). The table MerchantUser includes a Serial field, which the Examiner presumably equates to the claimed unique user key; this table relates to the distribution process. However, the Examiner subsequently refers to the "unique user key" as generated by the conditional access agent 28, associated with the delivery process, for a supposed teaching of "wherein the **unique user key is transmitted by a user application tool installed in the user terminal for authentication.**" In the context of the delivery process, *Fransdonk* does not in fact describe how this "unique user key" is generated, but that it simply is.

In the light of the above discussion, Applicants respectfully request that the rejection under § 102 be withdrawn, as anticipation under 35 U.S.C. 102 requires that each and every element of the claim be disclosed in a prior art reference. Based on the foregoing, it is clear that prior art does not anticipate independent claim 24 and dependent claim 39. Accordingly, claim 24 and corresponding dependent claims 25, 26 and 39 should be indicated as allowable at least for their dependencies on independent claims.

Favorable consideration is respectfully requested. If any unresolved issues remain, it is respectfully requested that the Examiner telephone the undersigned attorney at (703) 519-9955 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

DITTHAVONG MORI & STEINER, P.C.

8/27/2007
Date

Sangwon Kim
Attorney/Agent for Applicant(s)
Reg. No. 54221

Phouphanomketh Ditthavong
Attorney/Agent for Applicant(s)
Reg. No. 44658

918 Prince Street
Alexandria, VA 22314
Tel. (703) 519-9952
Fax. (703) 519-9958